UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

The property located at 500 W Bradley Rd., Apartment 301B, Fox Point, WI 53217. See Attachment A.

Case No. 19-M-114 (DEJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

The property located at 500 W Bradley Rd., Apartment 301B, Fox Point, WI 53217. See Attachment A.

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B.

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ evidence of a crime;
- □ contraband, fruits of crime, or other items illegally possessed;
- ■ property designed for use, intended for use, or used in committing a crime;
- □ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: 18 U.S.C. §§ 1030, 1343, and 371

The application is based on these facts: See attached affidavit.

□ Delayed notice of _______ days (give exact ending date if more than 30 days:_______________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Brett Lerner, FBI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: May 30, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Brett Lerner, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 500 W Bradley Rd, Apartment 301B, Fox Point, WI 53217, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am employed as a Special Agent with the FBI. I have been employed with the FBI since June 2014, and have been a Special Agent since September 2017. I am currently assigned to the FBI Milwaukee Division's Cyber Crime Task Force. As a Special Agent with the FBI, I investigate criminal computer intrusion matters involving botnets, distributed denial of service attacks, the distribution of "spam," the use of malware, identity theft, and other computer-based fraud. Prior to becoming a Special Agent, I worked for the FBI as a Staff Operations Specialist for approximately three years. In that position, I provided tactical analysis support to Special Agents working on national security cyber investigations.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. As described herein, the FBI has been investigating "booter" and "stresser" services for violations of federal law, including Title 18, United States Code, Sections 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer), 1343 (Wire Fraud), and 371 (Conspiracy to Violate Federal Law). At issue here is the service found at the domain "booter.ninja," which was operated by Luke Koltun, DOB 09/07/1999, until it was seized by the FBI on December 17, 2018, pursuant to a seizure warrant issued on that day by the U.S. District Court of the Central District of California.

Summary of Relevant Computer and Internet Concepts.

5. The information provided below regarding relevant computer and internet concepts is set forth based on my training, experience, and information provided to me by other members of law enforcement and knowledgeable witnesses:

6. "Internet Protocol address" or "IP address" is a unique numeric address used to identify computers on the Internet. The standard format[1] for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g.,

[1] IP version 4, or "IPv4", is the version of IP most commonly used today, and is the version described above. A newer version of the protocol, "IPv6", wholly different in appearance to IPv4, is sometimes used, but does not pertain to this request.

149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. Internet Service Providers ("ISPs") assign IP addresses to their customers' computers. ISPs typically log their customers' connections, allowing them to identify which of their customers was assigned a specific IP address during a particular session.

7. "Domain Names" serve to identify Internet resources, such as computers, networks, and services, with a text-based label that is easier to memorize than an IP address. A domain name consists of one or more parts (or "labels") that are conventionally concatenated and delimited by dots, such as example.com. The right-most label conveys the top-level domain; for example, the domain name www.example.com belongs to the top-level domain ".com."

8. "Server" is a centralized computer that provides services for other computers connected to it through a network. The computers that use the server's services are sometimes called "clients." Server computers can be physically located anywhere. For example, it is not uncommon for a network's server to be located hundreds, or even thousands of miles away from the client computers.

9. "Name Servers" are server applications that function like a phonebook. Name Servers will accept queries for domain names (such as example.com) and return an IP address associated with the domain, much as the name John Doe might be looked up in a telephone book to determine the corresponding telephone number.

10. "Registries" are companies responsible for managing the assignment of domains to IP addresses within a top-level domain. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which has its headquarters at 12061 Bluemont Way, Reston, Virginia.

11. "Registrars" sell domain names, and thus act as the intermediary between the registry and the purchaser of a domain name, who is known as the "registrant."

12. "Distributed Denial of Service" attacks, or "DDoS" attacks, are a type of network attack in which multiple Internet-enabled devices are used to attack computers for the purpose of rendering them inaccessible to legitimate users or unable to communicate with the Internet. One form of DDoS attack used in this investigation is the flooding of a website or server with internet traffic that makes the targeted website unable to be accessed by legitimate users or customers.

13. "Booter" or "Stresser" services are a class of DDoS attack tools characterized by their accessibility and affordability. These attacks are so named because they result in the "booting" or "dropping" of the victim-targeted website from the Internet. As described in more detail below, these attacks operate by flooding the victim-targeted website with tremendously high volumes of unsolicited traffic, effectively preventing the victim-targeted website from responding to normal traffic and from using the Internet.

Background of FBI Investigation into Booter/Stresser Services.

14. The FBI has been investigating the use of "booter" and "stresser" services that are often used to direct floods of misappropriated Internet traffic to unwitting victims for the purpose of preventing the victims from properly using the Internet, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) (Unauthorized Impairment of a Protected Computer) and 1343 (Wire Fraud), and conspiracy to commit the same, in violation of Title 18, United States Code, Section 371.

15. As part of this investigation, on December 17, 2018, an FBI agent applied for a seizure warrant in the U.S. District Court for the Central District of California to seize several booter and stresser services, including booter.ninja. That

warrant was executed that same day. The investigation that preceded issuance of that seizure warrant is summarized herein, with additional focus on booter.ninja.

16. Booter-based DDoS attack tools represent an effective advance in Internet attack technology because they are easy to use. For instance, the rates charged to customers by booter services vary according to the specific service, the desired "bandwidth" or attack size, the attack type, and the number of "concurrent" attacks allowed. For example, a premium, or "VIP," account on a given booter service might cost $100 a month and allow access to ten or more attack types, a peak attack bandwidth of 30 Gbit/s[2], and the ability to attack up to four IP addresses at one time. A "basic" plan might cost $25 to $35 a month and provide a more limited number of attack types, while allowing the customer to attack only a single IP address at a time.

17. The types of DDoS attacks offered by many booter sites tend to be Reflective Amplification Attacks ("RAA"). In general, RAA DDoS attacks function as follows:

[2] Gbit/s, or Gigabits per second, is a volumetric measure of network data. An average US domestic cable Internet subscriber might experience speeds of 10-50 Megabits per second (Mbit/s). One Gigabit is equivalent to 1000 Megabits.

a. First, the attacker learns the victim's IP address. This can be done through a variety of methods, including "resolvers" offered by the DDoS-for-hire sites themselves. These resolvers can discover, for example, the true IP associated with a web server so that an attack can bypass anti- DDoS defenses such as Cloudflare, determine on which IP address a given website or domain is hosted, or determine an IP address associated with a given Skype username. This was true for booter.ninja, as described below.

b. Second, the attacker chooses a "protocol," i.e., a type of communication between computers, which enables the attacker to send a very small request to a neutral third party and get a very large response. There are several Internet services that – though created for legitimate purposes – are commonly misused by booter services to create large RAA DDoS attacks. Examples include SSDP, also known as Simple Service Discovery Protocol, which allows for the advertisement and discovery of network services; NTP, or Network Time Protocol, which allows clock synchronization between computer systems; DNS, or Domain Name System, which facilitates the translation of domain names to IP addresses; and Chargen, or Character Generation Protocol, which facilitates testing and debugging. As described below, booter.ninja offered several different attack methods.

c. Third, the attacker crafts and sends such a request, but in doing so "spoofs" the request's origin: rather than using the attacker's own IP address, the attacker falsifies the victim's IP as the source, thus ensuring that the victim, rather than the attacker, receives the resulting flood of data from the protocol request.

d. Fourth, the neutral third party receives the request and is tricked by the "spoofed" origin IP – the third party returns its much larger response not to the attacker, but to the victim.

e. The attacker then replicates this process many times a second, often using many different third parties to reflect and amplify the attack, hence the name "Reflective Amplification Attack."

f. As a result, the victim receives an overwhelming amount of unsolicited Internet traffic, saturating its ability to communicate, and effectively taking it offline for the duration of the attack.

18. RAA DDoS attacks, as described above, are characterized by amplification factors—the size of the response data relative to the given query. For example, issuing the command "dig ns fbi.gov", a single line of query, results in

approximately 20 lines of text returned from the third party "reflector" service. This command/query can thus be said to have an amplification factor of approximately twenty. Using similar procedures, RAAs magnify the bandwidth available for attack by factors of 10, 20, 100, and even more. By doing so, RAAs appropriate bandwidth resources from the third-party reflectors, resources that the attacker does not pay for, and which far exceed "normal" use of those third parties, offloading the costs of RAAs to those third party servers and their upstream providers.

19. Further, as described above, an additional essential component of RAA is fraudulent misdirection. It does the attacker no good if the requested data is directed back to the attacker. The "spoofing" of the victim IP address is a central component of the attacks conducted by the booter services being investigated by the FBI.

20. The last component of an RAA is one of distribution. Instead of issuing the query to a single third party reflector, the query may be issued to hundreds or thousands of such third party reflectors simultaneously, each of which return with "amplified" responses. The resulting deluge of attack data saturates the network connection of the victim target website.

21. The FBI conducted testing of numerous booter/stresser sites, including booter.ninja, as part of its overall investigation into booters and stressers. While

testing the various booter services, the FBI usually purchased the cheapest attack plans available, merely to determine whether their attack functionality could be verified. That testing showed that these services could achieve attack volumes up to 25 to 30 Gbit/s. However, many of the services advertised the ability to perform much higher volume attacks, typically in the range of 50 Gbit/s but sometimes as high as 200 Gbit/s. Even at the lower volumes, the simultaneous use of two such services, at a combined cost of under $50/month, could result in an Internet outage for up to 10,000 ISP customers, for as long as the attacker wanted to implement the attack.

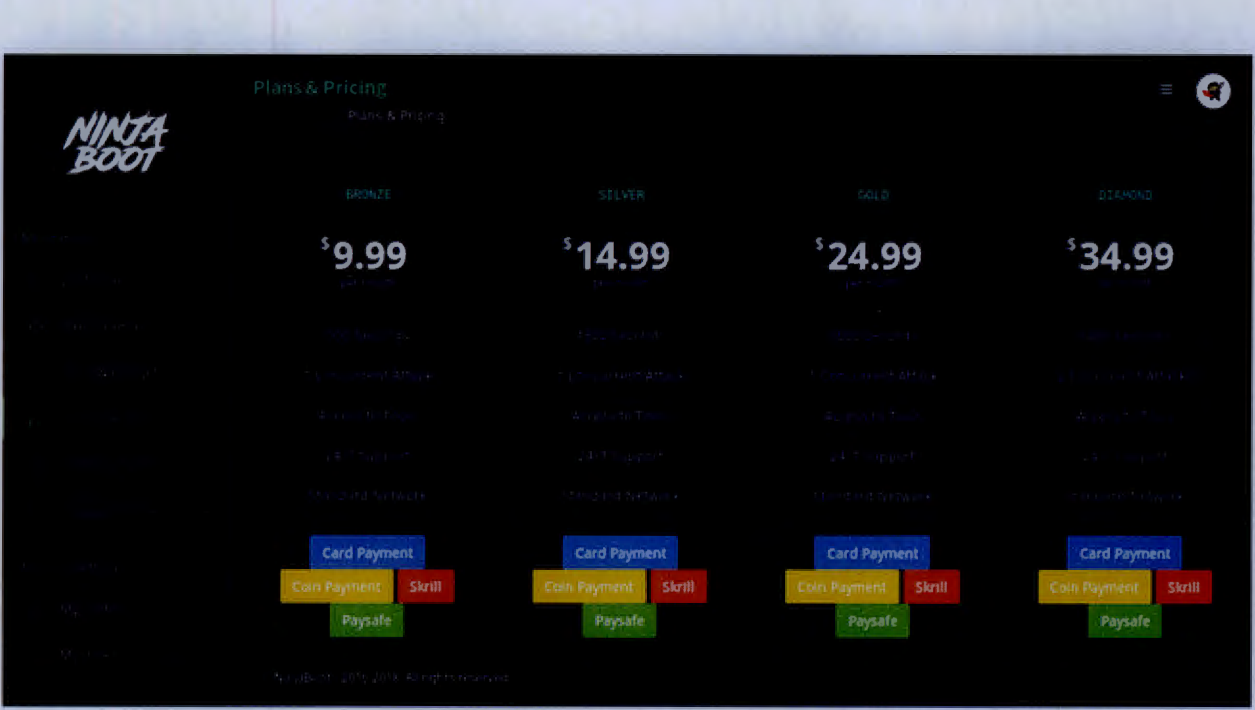
22. It is common for booter services to offer some token language within their Terms of Service or elsewhere that attempts to absolve the booter service from responsibility for attacks launched by their customers. However, based on my training, experience, and information provided by other members of law enforcement, I understand that the use of such language is largely pretext. Because RAA DDoS attacks by definition rely upon external services to act as "amplifiers," they must flood traffic to those external services en route to the victim, impairing and degrading the capacity of those services, for which they have received no permission. Furthermore, many of the booter services offered tools known as "resolvers." As described above, the purpose of "resolvers" is to obtain the IP

address of a victim and would be unnecessary if any customer was targeting their own infrastructure.

Facts Specific to booter.ninja.

23. As noted above, many booter services offer rates to customers based on specific types of service, attack type, attack size, and number of concurrent attacks allowed. Booter.ninja fit this mold. On its "purchase plan" page, booter.ninja advertised four types of plans (Bronze, Silver, Gold, and Diamond), ranging from $9.99 to $34.99. The $9.99 plan offered service for 900 seconds and one concurrent attack. The $34.99 plan, by contrast, offered service for 5400 seconds and two concurrent attacks. A screenshot of pricing for booter.ninja is below:

Figure 1: Screenshot of booter.ninja "Purchase Plan" page



Plans & Pricing

Plans & Pricing

BRONZE	SILVER	GOLD	DIAMOND
$9.99	$14.99	$24.99	$34.99
[illegible]	[illegible]	[illegible]	[illegible]
1 Concurrent Attack	1 Concurrent Attack	1 Concurrent Attack	1 Concurrent Attack
Access to Tools	Access to Tools	Access to Tools	Access to Tools
24/7 Support	24/7 Support	24/7 Support	24/7 Support
Standard Network	Standard Network	Standard Network	Standard Network

NinjaBoot 2015-2018 All rights reserved

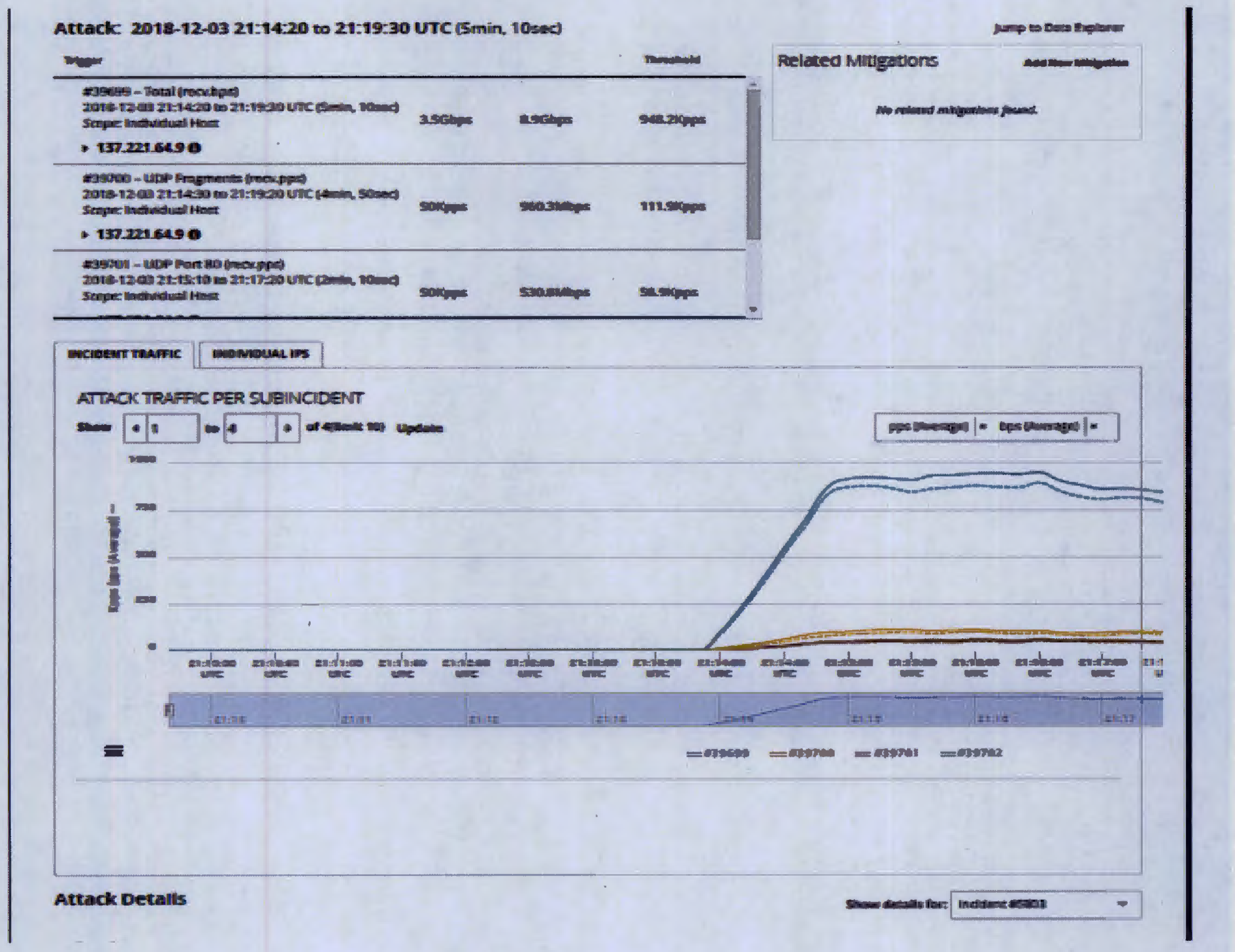
24. Booter.ninja advertised its services in a video posted on YouTube, which, according to the YouTube page, was produced and uploaded by booter.ninja on November 27, 2018. The 57-second video is titled "booter.ninja II Tutorial How to Boot! (In 60 Seconds!)," and available at www.youtube.com/watch?v=6jL2jsmLNZY (last viewed April 17, 2019). The video depicts the booter.ninja website and includes a voiceover by "Ninja" that walks the viewer through the service: how to add an IP address, scan for open ports, choose an attack method (SSDP, LDAP, DNS, LAG, NTP, Chargen, etc.), and then execute the attack to, according to the voiceover, "send your target to hell!" The video includes a closing (pretextual) statement that the service is "to be used for personal stress tests only."

25. The video shows that booter.ninja offers several tools designed to better facilitate a user's ability to conduct DDoS attacks. This includes tools such as "Domain Resolver," "Cloudflare Resolver," and "Skype Resolver." As described above, "resolvers" assist the attacker in learning the victim's IP address. "Cloudflare Resolver" tools attempt to resolve Cloudflare IPs, that is, discover the true IP associated with a web server so that the DDoS attack can bypass Cloudflare defenses. "Skype Resolver" tools help determine an IP address associated with a given Skype username. Based on my training and experience, as well as information provided to me by other members of law enforcement, I know that such resolving tools are part and parcel of criminal DDoS services.

26. The YouTube video page for this advertisement included several "comments." One commenter with the username "FBI Surveillance Van" asked a technical question about identifying ports, to which user "Saints Gaming" provided a detailed response regarding the use and capabilities of booter.ninja. Based on the content of the response, as well as my personal investigation into this service, I believe the user "Saints Gaming" was an administrator for booter.ninja. Further, as described below, the moniker "Saints Gaming" is similar to "Saint4145," which is linked to Luke Koltun.

27. As part of the investigation, the FBI purchased a subscription to booter.ninja in order to conduct a test of its capabilities. In December 2018, the FBI used the service to purposefully attack an FBI controlled IP address, determine the amount of traffic that emanated from booter.ninja provided services, and prove that booter.ninja was capable of the services it advertised. The results of the test show an attack volume of about 8.9 Gbps was generated by booter.ninja to the FBI controlled IP address. (The attack volume is an estimate only, and does not necessarily reflect the full volume of the attack traffic initiated.) A screenshot of the test results is included below as Figure 2. In sum, the FBI determined that booter.ninja successfully provided DDoS services capable of delivering, either solely or through concurrent use of other such services, sufficient attack volume to saturate a typical commercial Internet connection. This indicates a sizeable attack volume, as the bandwidth of a typical commercial Internet connection usually exceeds that of a residential connection.

Figure 2: A screenshot showing the attack volume of booter.ninja against a FBI controlled IP address for testing purposes.



Attack: 2018-12-03 21:14:20 to 21:19:30 UTC (5min, 10sec)

Jump to Data Explorer

Trigger			Threshold
#39699 – Total (recv.bps) 2018-12-03 21:14:20 to 21:19:30 UTC (5min, 10sec) Scope: Individual Host ▸ 137.221.64.9	3.5Gbps	8.9Gbps	948.2Kpps
#39700 – UDP Fragments (recv.pps) 2018-12-03 21:14:30 to 21:19:20 UTC (4min, 50sec) Scope: Individual Host ▸ 137.221.64.9	50Kpps	980.3Mbps	111.9Kpps
#39701 – UDP Port 80 (recv.pps) 2018-12-03 21:15:10 to 21:17:20 UTC (2min, 10sec) Scope: Individual Host	50Kpps	530.8Mbps	58.9Kpps

Related Mitigations

Add New Mitigation

No related mitigations found.

INCIDENT TRAFFIC | INDIVIDUAL IPS

ATTACK TRAFFIC PER SUBINCIDENT

Show 1 to 4 of 4(limit 10) Update

pps (Average) | bps (Average)

Attack Details

Show details for: Incident #[illegible]

28. As part of the investigation, I downloaded and reviewed database information from booter.ninja that was leaked and posted to an online forum in or around August 2017. The leaked information was stored as .txt files and displayed so that a reader could see and read the following tables, also known as logs: users (customers), customer "tickets" to the administrators, administrator "Replies" to customer's tickets, IP addresses associated with users, dashboard messages to all

users, various prices for services, and websites that were whitelisted and blacklisted for security purposes.

29. In reviewing these logs, I was able to identify three nicknames used by likely administrators of booter.ninja who responded to customer "tickets": "saint4145," "Francisco," and "Bero." In multiple instances, "Francisco" and "saint4145" replied to individuals who stated that they were interested in conducting a DDOS attack on IP addresses. For example, the user "CashThief" wrote a ticket to booter.ninja with the following complaint:

> People not going offline [the DDOS attack was not working][3]. Issue: ok, so everytime [sic] I hit someone off [use booter.ninja to target an IP address for a DDOS attack] they don't go offline. I tryed [sic] this on myself and I didnt [sic] go offline. I did the IP [address] then the port as 80 [internet traffic], then I did DNS, idk [I don't know] why but they aren't going offline if there is something wrong with the system. Thank you."

[3] At various point in this affidavit, I offer my interpretation of certain quoted conversations and the meaning of the certain terms in brackets. My interpretation of these conversations is based on my knowledge of this investigation to date, my experience and familiarity with these types of investigations, and open source information on the internet. The summaries of conversations do not include all potentially criminal conversations during this investigation, or all statements or topics covered during the course of the conversation. All quoted conversations in this affidavit do not represent finalized transcripts and may not represent the entire conversation that occurred between the identified individuals.

In response, "Francisco" wrote: "I was looking through your attack logs, and I saw the IP 84.104.51.199[4] [records showed that CashThief tried to attack IP address 84.104.51.199]. Therefore I tried to attack it [IP address 84.104.51.199], and it went offline [became inaccessible]." In separate message to a user, "Francisco" wrote: "Yes, you can make a home connection go offline." In another instance where administrators are conversing with customers regarding different attack methods, "Bero" wrote: "Should be working better now, try using LDAP or NTP, DNS is still having some issues." LDAP, NTP, and DNS are various attack methods that can be used in a booter/stresser attack.

Identification of Luke Koltun and the Premises

30. According to publically available domain registration information, the domain booter.ninja was assigned to IP addresses 104.25.228.29 and 104.25.229.29, and was hosted on servers owned and controlled by CloudFlare, Inc. Based on my training and experience, and publicly available information found on CloudFlare.com, I know CloudFlare offers a variety of network products and solutions, including web-hosting services.

[4] According to information obtained through centralops.net, IP address 84.104.51.199 has been owned and controlled by a company based in the Netherlands since 2011.

31. In April 2018, a subpoena was served on CloudFlare for records related to the domain booter.ninja. In response to the subpoena, CloudFlare stated booter.ninja is registered to Luke Koltun, email address luke.koltun@XXXXX.com, cell phone number 414-XXX-XX95, and billing address XXXXX N Range Line Road, Mequon, WI. Records checks for XXXXX N Range Line Road, Mequon, WI shows that the occupants of the house are T.K. and M.T. Based on records checks, it appears that T.K. is the mother of Luke Koltun.

32. In August 2018, a subpoena was served on PayPal for records related to PayPal account XXXXXXXXXXXXXX75100. In response to the subpoena, PayPal stated that the account was held in the name "Luke Koltun" with email address luke.koltun@XXXXX.com, and addresses of both XXXXX N Range Line Road, Mequon, WI, and 500 W Bradley Rd., Apartment 301B, Fox Point, WI, 53217 (the PREMISES). Transaction data from the PayPal account showed numerous payments for services that are consistent with the services offered by booter.ninja. For example, the records showed payments for "1 Month 500 Seconds" for $5.00USD, "Trial Boot – 1 Day" for $1.00USD, and "1 Months for 1000 Seconds" for $10.00USD. The PayPal records also showed that the account was also tied to Wells Fargo Bank, NA, checking account number XXXXXX5393.

33. In August 2018, a subpoena was served on Wells Fargo for records related to bank account number XXXXX5393. In response to the subpoena, Wells Fargo produced records showing that the account is in the name of Luke Koltun with an address the PREMISES. The records show that in June 2018, Luke Koltun made a recurring subscription payment of $18.06 to www.namecheap.com. A review of publically available information shows that namecheap.com is a domain name registration service that booter.ninja utilized.

34. In August 2018, a subpoena was issued to NameCheap for records related to Luke Koltun and the domain booter.ninja. In response to the subpoena, NameCheap produced records showing that Luke Koltun, email address luke.koltun@XXXX.com, and address XXXXX N Range Line Road, Mequon, WI, was listed as the registrant, administrative contact, technical contact, and billing contact for several domains including booter.ninja. The domain booter.ninja was registered on October 18, 2016, and the registration is set to expire on October 18, 2019. The NameCheap records also shows that Luke Koltun's user name to access his NameCheap account was "Saint4145," which was the same alias used by a booter.ninja administrator in the logs described above.

35. Records indicate that Luke Koltun is currently a 19-year old high school student with ties to two residences; his mother's residence at XXXXX N

Range Line Road, Mequon, WI; and his father's residence, the PREMISES, 500 W Bradley Rd. Apartment 301B, Fox Point, WI, 53217. As described herein, the investigation revealed that the PREMISES is Koltun's primary residence. Law enforcement agents conducted physical surveillance of Koltun and his family members on several occasions. The surveillance showed Koltun going to and from the PREMISES on a regular basis. During the surveillance period, agents did not observe Koltun travel to or from his mother's residence.

36. Specifically, on March 21, 2019, at around 4 p.m., FBI surveillance specialists observed K.K. (Koltun's father) pick up Koltun from the Nicolet Recreation Department, collocated with Nicolet High School, and drive back to the PREMISES. That same day, around 4:19 p.m., surveillance specialists observed Koltun driving a Blue 2016 Subaru Crosstrek with the license plate Wisconsin 528ZBL, which was registered to K.K. at the PREMISES. Koltun drove the car from the PREMISES for an unknown purposes, and later returned to the PREMISES and parked the car at around 4:31 p.m. Koltun was not observed outside of the PREMISES for the rest of the day. On Friday, March 29, 2019, around 12:45 p.m., surveillance specialists observed Koltun driving the Subaru Crosstrek and enter the underground parking garage at the PREMISES. On Thursday, April 4, 2019, around 5:06 p.m., surveillance specialists observed Koltun as a passenger in the

Subaru Crosstrek, with K.K. driving, as the vehicle proceeded to the underground parking garage of the PREMISES. On April 29, 2019, surveillance specialists began surveillance of the PREMISES around 5 a.m., and around 6:40 a.m., they observed Koltun exist the PREMISES and enter the most southern building of the apartment complex. A few minutes later, around 6:46 a.m., surveillance specialists observed Koltun exit the apartment complex and enter a yellow school bus, which then proceeded to Nicolet High School, 6701 North Jean Nicolet Rd, Glendale, WI 53217. On May 6, 2019, around 4:24 p.m., surveillance specialists observed Koltun exit Nicolet High School and enter the passenger side of the Subaru Crosstrek, which was being driven by K.K. They drove back to the PREMISES. Surveillance specialists maintained surveillance of the PREMISES that evening; they observed the apartment lights go out around 9:00 p.m., and ultimately discontinued surveillance around 10:18 p.m. During this time, surveillance specialists did not observe Koltun leave the PREMISES.

37. Based on my training and experiences, I know that electronic devices such as desktops, laptops, cell phones, and financial receipts are usually kept at the primary residence of the devices' owner. And, as described herein and based on my personal involvement in this investigation, I believe that the electronic devices Luke Koltun used to operate and administer booter.ninja will be found at the PREMISES.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

38. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

39. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as

direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to operate a website that is used for illegal conduct, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

41. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media.

Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

42. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

43. Because multiple people share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly

used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

44. *Unlocking Apple brand devices:* I know based on my training and experience, as well as from information found in publicly available materials including those published by Apple, that Apple devices are used by many people in the United States, and that some models of Apple devices such as iPhones and iPads offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID.

a. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

b. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

c. If Touch ID enabled Apple devices are found during a search of the PREMISES, the passcode or password that would unlock such the devices are presently unknown to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) of any Apple device(s) found during the search of the PREMISES to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant Apple device(s) via Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

d. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the premises to press their finger(s) against the Touch ID sensor of the locked Apple device(s) found during the search of the PREMISES in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID.

e. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the Apple device(s) found in the PREMISES as described above within the five attempts permitted by Touch ID, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

f. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the PREMISES to the Touch ID sensor of the Apple brand device(s), such as an iPhone or iPad, found at the PREMISES for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

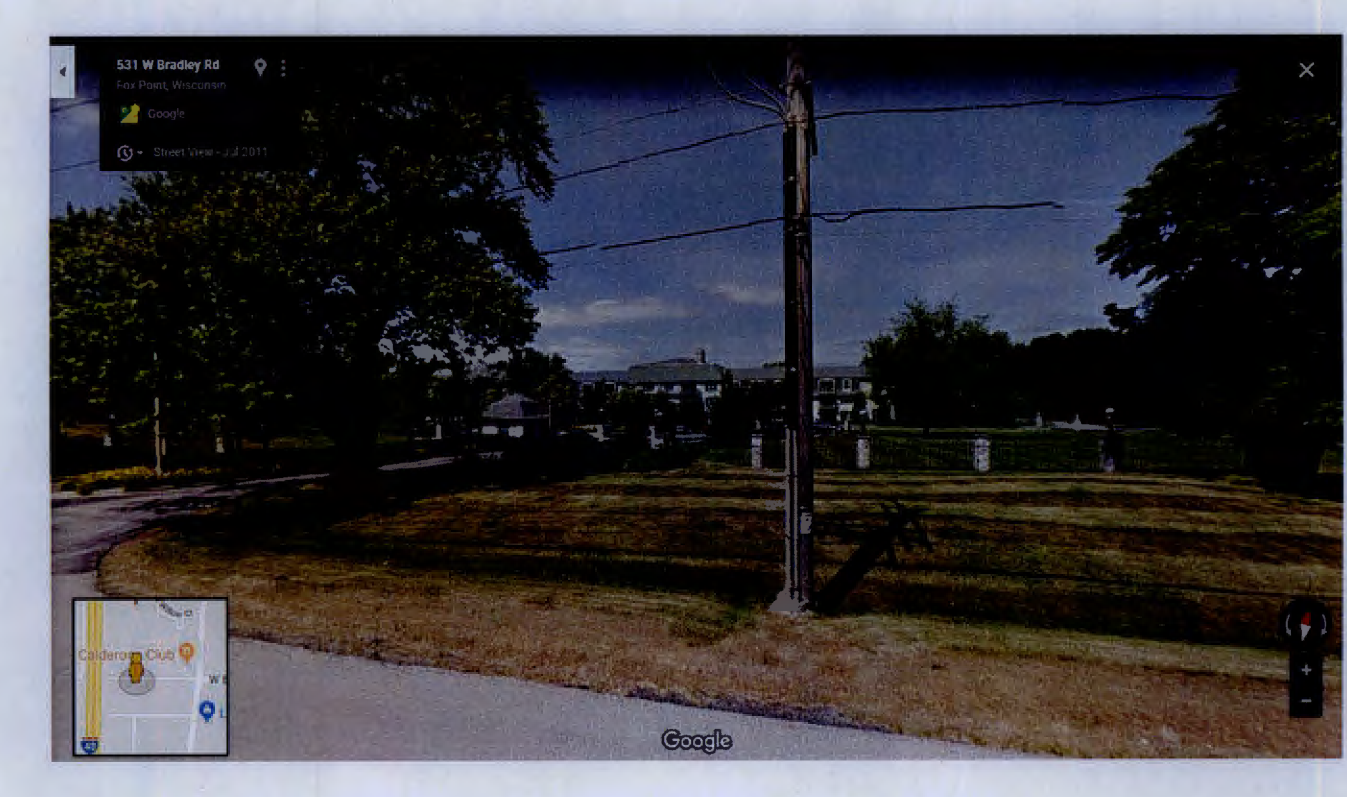
CONCLUSION

45. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

ATTACHMENT A

Property to be searched

The property to be searched is 500 W Bradley Rd., Apartment 301B, Fox Point, WI 53217, as shown below:



ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 1030(a)(5)(A) (unauthorized impairment of a protected computer), 1343 (wire fraud), and 371 (conspiracy to violate federal law), those violations involving Luke Koltun and occurring after October 18, 2016, including:

a. Records and information relating to the development, administration, and operation of booter.ninja;

b. Records and information relating to stresser/booter services and tools;

c. Records and information relating to website development, administration, and operation;

d. Records and information relating to the identity or location of the Luke Koltun and accomplices involved in booter/stresser services, including booter.ninja;

e. Bank account records, loan documents, wire transfer records, money order receipts, postal express mail envelopes, bank statements, safe deposit box keys and records, money containers, financial records or notes showing payment, receipt, concealment, transfer, or movement of money generated from booter.ninja or other booter/stresser services, or financial transactions related to such activities, including any virtual or crypto currency;

f. Records of off-site storage locations including but not limited to safe deposit box keys and records, and records and receipts and rental agreements for storage facilities;

g. Records and information showing occupancy.

2. Computers or storage media used as a means to commit the violations described above.

3. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of individuals found at the premises to the Touch ID sensor of Apple brand device(s), such as an iPhone or iPad, found at the premises for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.